COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021
Tel 212 434 9400 Fax 212 434 9875

"The Ongoing Neglect of Maritime Transportation Security"

Written Testimony before

a hearing of the

Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure

United States House of Representatives

on

"The 9/11 Commission's Maritime Transportation Security Proposals"

by

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies

Room 2167
Rayburn House Office Building
Washington, D.C.

2:00 p.m.
August 25, 2004

"The Ongoing Neglect of Maritime Transportation Security"

by
Stephen E. Flynn
Jeane J. Kirkpatrick Senior Fellow
For National Security Studies

Chairman LoBiondo and distinguished members of the House Subcommittee on Coast Guard and Maritime Transportation. I am the Jeane J. Kirkpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations. I am honored to be appearing before you this morning to discuss the vitally important issue of maritime transportation security. This has been a topic that has been a focus of my professional life for better part of a decade. As I have testified on eight occasions over the past three year, I believe maritime transportation is one of our nation's most serious vulnerabilities, and we are simply not doing enough to respond to the terrorist threat to this critical sector.

The nation owes an enormous debt of gratitude to the commissioners and the dedicated staff of the 9/11 Commission. Their report should serve as an antidote for anyone in Washington who thinks that we can afford to take a business-as-usual approach to confronting the threat of catastrophic terrorism. From my perspective, the report makes three central points central to understanding our post-9/11 world. First, that the attacks on New York and Washington were a meticulously planned and executed campaign directed by a tenacious enemy intent on exploiting America's most glaring vulnerability—its largely unprotected homefront. Second, prior to 9/11, the U.S. government was neither focused on nor effectively organized to confront this threat—and that neither Democrats nor Republicans are blameless for that unhappy state of affairs. Third, that despite the horror of that day and the passing of nearly three years, there is much work to be done towards making the critical infrastructure that underpins U.S. power less of a soft target.

I would be less than candid if I did not acknowledge that the hearing today sparks within me a sense of déjà vu. Prior to 9/11 I had the privilege to work with former Senators Gary Hart and Warren Rudman and the U.S. Commission on National Security/21st Century. As the members of this committee know, that commission concluded after three years of study in its final report released in January 2001, that the greatest national security challenge for the United State was the threat of catastrophic terrorism and that the federal government was not organized to confront that threat. Like the 9/11 Commission, the Hart-Rudman Commission was a blue-ribbon, bipartisan group chartered by Congress. Unfortunately, in our case, that did not prevent Washington from largely ignoring the report. This hearing and the others underway this month when Congress is usually in recess suggests that things may be different this time around. For the sake of our nation, I certainly hope that this will be the case, and that the recommendations of this Commission will be acted upon with dispatch.

I am confident that the 9/11 Commission would readily acknowledge that, had they had more time, one of the areas they would have spent it is on would have been in

fleshing out their recommendations for improving transportation security specifically, and critical infrastructure protection more generally. This is not the strongest part of their report. Still, the Commission has performed a valuable service by documenting:

(1) That during the decade before September 11, 2001, counter-terrorism measures as a part of border security was not seen as a national security matter and were largely neglected.

(2) That there remains a serious lack of balance in our investment in protecting the transportation sector with over ninety percent of the nation's annual investment in TSA going to aviation—and virtually all of that has been dedicated to only passenger security.

(3) That the risk of harm is great or greater in the maritime and surface transportation modes.

(4) That TSA still not has developed an integrated strategic plan for the transportation sector nor has it developed plans to protect the individual modes of transportation.

Based on my assessment of the state of transportation security both before and since 9/11, I agree with all these findings. I would add to that list my concern that many of the helpful measures being pursued by the administration in the area of maritime transportation security are not being adequately resourced to address the threat to this sector. Specifically, in my testimony today, I will point out the critical shortcomings in the major post-9/11 security initiatives that deserve the immediate attention of the White House and the Congress.

Officially July 1, 2004 marked the dawning of a new age for maritime security. The International Ship and Port Facility Security Code (ISPS) is now in force. 22,539 vessels that ply the seas and the 7,974 port facilities that serve as their on-ramps and off-ramps should be abiding by new security measures adopted by the International Maritime Organization in December 2001. Congress gave the code the force of law when it adopted the Maritime Transportation Security Act of 2002. But the new mandate has not come with the resources required to meet it. Since 9/11 Washington has provided only $516 million dollars towards the $5.6 billion the Coast Guard estimates U.S. ports need to make them minimally secure. In the FY2005 budget, the White House asked for just $50 million more. Given the severe constraints on the state and local budgets within the jurisdictions where America's commercial seaports are located, it is difficult to see how these ports are in any position to bankroll the new security requirements that have been thrust upon them.

Congress also failed to authorize new funding to pay for staffing and training Coast Guard inspectors to verify that everyone is following the new rules. This is so even though the Maritime Transportation Security Act mandates that the Department of Homeland Security certify annually that ports and ships engaged in commerce with the United States are compliant with the code. The evidence to date is that much of the international maritime community is simply going through the motions. On the day the

ISPS code went into force, only one-half of the world's port facilities had gotten around to submitting their security plans—and most were thrown together in the final weeks before the deadline. In the United States, according to a GAO report released on June 30th, every one of the 2,913 facility plans submitted to the Coast Guard in early 2004 were found to be deficient. Just 120 had undertaken the necessary remedial steps to secure approval by mid-June 2004.

The Coast Guard is coping with its new compliance mandate by marshalling small teams of reserve junior officers with limited experience in marine inspections and little to no background in security to do the first round of overseas inspections. I very much worry that this approach will send the wrong message to the international maritime community. A series of inconsistent and superficial inspections will communicate to port authorities at home and abroad that the U.S. government is not really that serious about maritime security. This will lead many to decide not to make the kinds of investments they should be making to bolster security. It will also discourage those who have shown a willingness to date to be forward-leaning if they discover others are getting by with making only token efforts.

The Coast Guard is not only struggling to carry out this new assignment, but its fleet of cutters and aircraft are being pushed to the breaking point and beyond to meet the combined imperatives of its traditional missions along with its new maritime homeland security mandate. This sub-committee needs no reminder that the Coast Guard is only slightly larger that the New York Police Department even though it bears the burden of being America's first line of defense along the 95,000 miles of shoreline and the over 3 million square miles of waters that are adjacent to U.S. maritime borders. It is patrolling the nation's coastal waters with vessels and airplanes that are operating long beyond their expected service life. The result is that the already dangerous job of performing these missions is being compounding by frequent engineering casualties that put the lives of Coast Guard men and women at risk. Just this month, one of the service's largest ships, the 378 cutter GALLETIN which was built in 1968, barely made it out of its homeport to escape Hurricane Charley when one of its main engines died. The lengthy twenty-plus year time table for replacing the Coast Guard's fleet with the Integrated Deepwater System is likely to leave the maritime environment increasingly exposed in the near term as the assets the Coast Guard now has fail far more quickly than they can be replaced. It is inexplicable to me that despite the war on terrorism, that the White House and Congress have been reluctant to accelerate its pre-9/11 schedule to modernize the Coast Guard's obsolete fleet.

Another much touted Coast Guard initiative for improving maritime security is the Automated Identification System (AIS) for tracking ships approaching and operating within U.S. ports and coastal waters. Most Americans are simply flummoxed when they learn that while the FAA can track planes flying throughout our airspace, the U.S. government currently has no means to do the same with ships. The AIS system being pursued by the Coast Guard widely misses the mark of rectifying that situation. Designed only to detect vessels within 20-30 miles of U.S. ports, the system does not provide adequate time to muster an effective response should a vessel pose a threat. This

is because most ocean-going vessels could cover that distance in 1-2 hours. We live in an age when GPS devices are being placed in cellular phones. It makes no sense why the U.S. government is not aggressively pursing a more ambitious satellite tracking system for monitoring vessel movements once they leave a foreign port and are destined for U.S. waters.

The Customs and Border Protection Directorate at the Department of Homeland Security shares with the Coast Guard the burden of securing the maritime transportation system. CBP has been the lead agency in addressing the risk that cargo containers might be used as a poor man's missile. It has undertaking a number of initiatives since 9/11, but here again the paucity of resources being dedicated to support these efforts leaves America dangerously vulnerable to another act of catastrophic terrorism.

The Container Security Initiative (CSI) is the centerpiece of the administration's effort in this area. This well conceived program involves placing U.S. customs inspectors overseas in the port of loading to target containers for inspection before they are loading on a ship destined for the United States. To date over 24 ports, including all the largest seaports in the world, have signed agreements to participate in the CSI program. That is the good news. The not so good news and that CBP is staffing the CSI program by sending teams of just four to eight inspectors on temporary duty assignments of three to four months duration because the administration has not authorized the overseas billets for longer assignments. Inspectors are receiving no formal language or other training to prepare them for these overseas postings. Given that the teams are so small—only eight inspectors in Hong Kong which is the world largest port, they are able to inspect only the tiniest of percentages of containers.

The companion piece to CSI is the "Customs-Trade Partnership Against Terrorism" or C-TPAT. Under C-TPAT, CBP has reached out to companies and carriers involved in importing goods into the United States. It has asked them to assess the vulnerabilities of their supply chains and to put in place measures to address any weaknesses that they discover. Companies that join C-TPAT enhance the odds that CBP will view them as low-risk shippers which translates into their conveyances or shipments not being subjected to routine examinations. Like CSI, the underlying logic of the program is laudable. Unfortunately, CBP is not adequately staffed to even review the nearly five thousand initial C-TPAT applications it has received. Worse still, they doing not have the manpower to provide an ongoing system that verifies that companies are actually taking tangible steps to bolster supply chain and transportation security. As a result, the regime is essentially, a "trust-but-don't-verify" approach.

What this means is that the maritime transportation system remains a very soft target for America's enemies to exploit. As we have learned from the intelligence that led to the most recent Orange alert on August 1, al Qaeda is committed to targeting critical infrastructure and is willing to invest considerable time and energy in staking it out and formulating complex plans to evade the security measures that are in place. I have little doubt that al Qaeda possesses the means to identify those users of the maritime transportation system that U.S. authorities currently view as low-security risks. I also

believe that they are fully capable of exploiting the many opportunities to intercept and compromise these legitimate shipments either at their point of origin or anywhere along the transportation route they travel. I am deeply concerned that despite the efforts made by the U.S. government to date; only an extraordinary instance of good luck would allow U.S. authorities to detect a compromised "low-risk" user in time to foil a terrorist attack.

All this sets us up for a possible worse-case scenario where we will have a terrorist incident involving a C-TPAT company, who ships their good from an ISPS certified port facility located in a port that is a participant in CSI, aboard an ISPS certified ship, that onloads its cargo on to a train or truck upon arrival in the United States, and then sets off a weapon of mass destruction in America's heartland. Our enemies will then successfully discredit the entire regime now in place. Since no shipment will be able to be viewed as low-risk, U.S. authorities will have to attempt to inspect all shipments while it scrambles to then put a credible, verifiable security regime in place. In the interim we could bring the U.S. economy and the entire international trade system to its knees.

In short, a token security effort in the maritime transportation sector may prove worse than making no effort at all. This is because it seduces the American people into having a false sense of security that forestalls making real investments in protecting our critical infrastructure. Further, it will almost certainly generate a severe loss of public confidence in the federal government when those measures are shown to have been entirely insufficient following a successful attack. Announcing ambitious security initiatives without providing adequate resources to make them credible is dangerous business. It practically assures that we will have future hearings like this one, where blue-ribbon commissions will be testifying that too little was done to secure Americans from the real and present danger of catastrophic terrorist attacks on the United States.

Thank you Mr. Chairman for this opportunity to testify before you on this very serious issue. I look forward to responding to your questions.